TREND MICRO

3.0

TREND MICRO™

Smart Protection Server

Installations- und Upgrade-Handbuch

Security Made Smarter

Endpoint Security Messaging Security Protected Cloud Web Security

TREND MICRO SMART PROTECTION NETWORK™

Trend Micro Incorporated behält sich das Recht vor, Änderungen an diesem Dokument und dem hierin beschriebenen Produkt/Service ohne Vorankündigung vorzunehmen. Lesen Sie vor der Installation und Verwendung des Produkts/Services die Readme-Dateien, die Anmerkungen zu dieser Version und die neueste Version der verfügbaren Benutzerdokumentation durch:

http://docs.trendmicro.com/de-de/home.aspx

Dokument-Nr.: APEM36293/140116

Release-Datum: März 2014

Geschützt durch U.S. Patent-Nr.: Zum Patent angemeldet.

Diese Dokumentation enthält eine Beschreibung der wesentlichen Funktionen des Produkts/Services und/oder Installationsanweisungen für eine Produktionsumgebung. Lesen Sie die Dokumentation vor der Installation oder Verwendung des Produkts/ Services aufmerksam durch.

Ausführliche Informationen über die Verwendung bestimmter Funktionen des Produkts/Services finden Sie im Trend Micro Online Help Center und/oder der Knowledge Base von Trend Micro.

Das Trend Micro Team ist stets bemüht, die Dokumentation zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder anderen Dokumenten von Trend Micro wenden Sie sich bitte an docs@trendmicro.com.

Bewerten Sie diese Dokumentation auf der folgenden Website:

http://www.trendmicro.com/download/documentation/rating.asp

Inhaltsverzeichnis

Vorwort

Kapitel 1: Installation und Upgrade von Smart Protection Servern planen

Kapitel 2: Smart Protection Server installieren und upgraden

Kapitel 3: Aufgaben nach der Installation

Kapitel 4: Hilfe anfordern

Stichwortverzeichnis

Vorwort

Vorwort

Willkommen beim Smart Protection Server™ Installations- und Upgrade-Handbuch. Dieses Dokument enthält Informationen über die Produkteinstellungen.

Es werden folgende Themen behandelt:

- *Info über Trend Micro auf Seite iv*
- *Produktdokumentation auf Seite iv*
- *Zielgruppe auf Seite iv*
- *Dokumentationskonventionen auf Seite v*

Info über Trend Micro

Trend Micro Incorporated bietet Sicherheitssoftware und -services für Virenschutz, Anti-Spam und Content-Filtering. Trend Micro hilft Kunden weltweit beim Schutz ihrer Computer vor bösartigem Code.

Produktdokumentation

Die Dokumentation zum Smart Protection Server besteht aus den folgenden Komponenten:

DOKUMENTATION	BESCHREIBUNG
Installations- und Upgrade-Handbuch	Unterstützt Sie bei der Planung der Installation, Upgrades und Verteilung.
Administratorhandbuch	Unterstützt Sie bei der Konfiguration aller Produkteinstellungen.
Online-Hilfe	Bietet detaillierte Anweisungen zu jedem Feld und dazu, wie Sie alle Funktionen mit Hilfe der Benutzeroberfläche konfigurieren.
Readme-Datei	Enthält die neuesten Informationen über ein Produkt, die möglicherweise nicht in der anderen Dokumentation zu finden sind. Zu den Themen gehören die Beschreibung von Funktionen, Tipps für die Installation, Lösungen bekannter Probleme und bereits veröffentlichte Produktversionen.

Die Dokumentation ist verfügbar unter folgender Adresse:

http://downloadcenter.trendmicro.com/?regs=DE

Zielgruppe

Die Dokumentation zum Smart Protection Server™ wurde für IT-Manager und Administratoren geschrieben. In dieser Dokumentation wird davon ausgegangen, dass der Leser fundierte Kenntnisse über Computernetzwerke besitzt.

Kenntnisse über Viren-/Malware-Schutz oder Spam-Abwehr-Technologien werden nicht vorausgesetzt.

Dokumentationskonventionen

Im Smart Protection Server™ Benutzerhandbuch gelten die folgenden Konventionen.

Tabelle 1. Dokumentationskonventionen

Konvention	Beschreibung
NUR GROSSBUCHSTABEN	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten und Optionen
Navigation > **Pfad**	Der Navigationspfad zu einem bestimmten Fenster **Datei** > **Speichern** bedeutet beispielsweise, dass Sie in der Benutzeroberfläche im Menü **Datei** auf **Speichern** klicken
Hinweis	Konfigurationshinweise
Tipp	Empfehlungen oder Vorschläge
Warnung!	Wichtige Aktionen und Konfigurationsoptionen

Kapitel 1

Installation und Upgrade von Smart Protection Servern planen

Dieses Kapitel enthält Informationen über die Planung einer Erstinstallation oder eines Upgrades von Trend Micro™ Smart Protection Server™.

Es werden folgende Themen behandelt:

Systemvoraussetzungen

In der folgenden Tabelle werden die Systemvoraussetzungen aufgeführt:

TABELLE 1-1. Systemvoraussetzungen

HARDWARE / SOFTWARE	VORAUSSETZUNGEN
Hardware	• 2,0 GHz Intel™ Core2 Duo™ 64-Bit-Prozessor mit Unterstützung von Intel™ Virtualization Technology™ oder gleichwertig • 2GB Arbeitsspeicher • 30 GB oder 35 GB (empfohlen) Festplattenspeicher bei Installation auf einer virtuellen Maschine **Hinweis** Der Smart Protection Server partitioniert den erkannten Festplattenspeicher nach Bedarf automatisch. **Hinweis** Das Protokoll "Gesperrter Internet-Zugriff" stoppt das Sammeln von Daten, wenn vom Smart Protection Server erkannt wird, dass der freie Speicherplatz unter 1 GB liegt. Sobald der Administrator mindestens 1,5 GB Speicher freigegeben hat, werden vom Smart Protection Server wieder Daten gesammelt. • Monitor mit einer Mindestauflösung von 1024 x 768 bei 256 Farben oder mehr

Hardware / Software	Voraussetzungen
Virtualisierung	• Microsoft™ Windows Server™ 2008 R2 Hyper-V™ **Hinweis** Installieren Sie den Legacy-Netzwerkadapter zur Erkennung des Netzwerkgeräts für Hyper-V-Installationen. Verwenden Sie nach der Installation des Smart Protection Servers die Befehlszeilenschnittstelle (CLI), um Hyper-V-Integrationskomponenten eine Erhöhung der Kapazität zu ermöglichen. • Microsoft™ Windows Server™ 2012 Hyper-V™ **Hinweis** Installieren Sie den Legacy-Netzwerkadapter zur Erkennung des Netzwerkgeräts für Hyper-V-Installationen. • VMware™ ESXi™ Server 5.5, 5.1, 5.0 Update 2, 4.1 Update 1, 4.0 Update 3 oder 3.5 Update 4 • VMware™ ESX™ Server 4.1 Update 1, 4.0 Update 3 oder 3.5 Update 4 • Citrix™ XenServer™ 6.2, 6.0 und 5.6 **Hinweis** Wenn Sie einen Citrix™ XenServer verwenden, erstellen Sie anhand der Vorlage **Anderen Datenträger installieren** eine neue virtuelle Maschine. **Hinweis** Ein speziell entwickeltes, gesichertes und leistungsoptimiertes 64-Bit-Linux-Betriebssystem ist Teil des Smart Protection Servers.

HARDWARE / SOFTWARE	VORAUSSETZUNGEN
Virtuelle Maschine	• CentOS 5 64 Bit (Gastbetriebssystem) • Wenn Ihre VMWare-Version (z. B. 3.5 und 4.0) CentOS nicht unterstützt, verwenden Sie Red Hat™ Enterprise Linux™ 5 64 Bit. **Hinweis** Nur Virtual NIC E1000- und VMware VMXNET3-NICs werden unterstützt. • 2GB Arbeitsspeicher • 2.0-GHz-Prozessor • 30 GB oder 35 GB (empfohlen) Festplattenspeicher bei Installation auf einer virtuellen Maschine • 1 Netzwerkgerät • Mindestens 2 virtuelle Prozessoren (4 virtuelle Prozessoren empfohlen) • Netzwerkgerät **Hinweis** Das Kernel-Modul von Smart Protection Server installiert das VMWare Tools-Modul vmxnet3. VMWare Tools müssen daher nach der Installation von Smart Protection Server nicht installiert werden. Wenn Sie während der Installation eine vmxnet3-NIC auswählen, wird möglicherweise die Meldung **Die Mindest-Hardwareanforderungen sind nicht erfüllt** angezeigt, da der vmxnet3-Treiber noch nicht installiert wurde. Diese Meldung kann ignoriert werden, und die Installation wird normal fortgesetzt.

Hardware / Software	Voraussetzungen
Webkonsole	• Microsoft™ Internet Explorer™ 7.0 oder höher mit aktuellen Updates • Mozilla™ Firefox™ 3.6.0 oder höher • Adobe™ Flash™ Player 8.0 oder höher ist für das Anzeigen von Diagrammen in Widgets erforderlich. • Mindestauflösung von 1024 x 768 bei 256 Farben oder mehr

Verteilung planen

Der folgende Abschnitt bietet Information darüber, wie Sie den Typ der zu konfigurierenden Umgebung ermitteln, wenn Sie lokale Smart Protection Server installieren.

Bewährte Methoden

- Vermeiden Sie es, gleichzeitig manuelle und zeitgesteuerte Suchvorgänge durchzuführen. Staffeln Sie die Suchvorgänge in Gruppen.
- Vermeiden Sie, dass alle Endpunkte gleichzeitig die Funktion Jetzt durchsuchen verwenden. Beispielsweise die Option **Nach dem Update 'Jetzt durchsuchen' ausführen**.
- Sie können mehrere Smart Protection Server installieren, um die Kontinuität des Schutzes sicherzustellen, falls die Verbindung zu einem Smart Protection Server nicht verfügbar ist.
- Passen Sie Smart Protection Server an langsamere Netzwerkverbindungen an, zirka 512KBit/s, indem Sie Änderungen in der `ptngrowth.ini`-Datei vornehmen.

Datei `ptngrowth.ini` konfigurieren

Prozedur

1. Öffnen Sie die Datei "ptngrowth.ini" in `/var/tmcss/conf/`.
2. Ändern Sie die `ptngrowth.ini`-Datei und verwenden Sie die unten empfohlenen Werte:

```
[COOLDOWN]
ENABLE=1
MAX_UPDATE_CONNECTION=1
UPDATE_WAIT_SECOND=360
```

3. Speichern Sie die `ptngrowth.ini`-Datei.
4. Geben Sie für den Neustart des lighttpd-Service den folgenden Befehl über die Befehlszeilenschnittstelle (CLI) ein:

```
service lighttpd restart
```

Richtlinien für die Verteilung

Berücksichtigen Sie Folgendes, wenn Sie einen lokalen Smart Protection Server einrichten:

- Smart Protection Server ist eine CPU-lastige Anwendung. Dies bedeutet, dass je mehr CPU-Ressourcen zur Verfügung stehen, desto mehr gleichzeitige Anforderungen verarbeitet werden können.
- Die Netzwerkbandbreite kann zu einem Engpass werden, abhängig von der Netzwerkinfrastruktur und der Anzahl gleichzeitiger Update-Anforderungen und Verbindungen.
- Bei einer großen Anzahl gleichzeitiger Verbindungen zwischen Smart Protection Server und Endpunkten ist möglicherweise mehr Arbeitsspeicher erforderlich.

Installation vorbereiten

Bei der Installation von Smart Protection Server wird Ihr vorhandenes System für die Programminstallation formatiert. Für eine Installation von VMware oder Hyper-V ist die Erstellung einer virtuellen Maschine vor der Installation erforderlich. Nachdem Sie die Anzahl der Smart Protection Server für Ihr Netzwerk ermittelt haben, können Sie mit der Installation beginnen.

Tipp

Sie können mehrere Smart Protection Server installieren, um die Kontinuität des Schutzes sicherzustellen, falls die Verbindung zu einem Smart Protection Server nicht verfügbar ist.

Sie benötigen für die Installation die folgenden Informationen:

- Angaben zum Proxy-Server
- Ein Server für eine virtuelle Maschine, der die Anforderungen Ihres Netzwerks erfüllt

Kapitel 2

Smart Protection Server installieren und upgraden

Dieses Kapitel enthält Informationen darüber, wie Sie einen Trend Micro™ Smart Protection Server™ installieren und Upgrades durchführen.

Es werden folgende Themen behandelt:

- *Eine Erstinstallation durchführen auf Seite 2-2*
- *Upgraden auf Seite 2-14*

Eine Erstinstallation durchführen

Starten Sie das Installationsprogramm, nachdem die Voraussetzungen zur Installation erfüllt sind, um mit der Installation zu beginnen.

Smart Protection Server installieren

Prozedur

1. Erstellen Sie auf Ihrem VMware- oder Hyper-V-Server eine virtuelle Maschine, und geben Sie an, dass die virtuelle Maschine vom ISO-Image von Smart Protection Server starten soll.

   Lesen Sie den Abschnitt "Virtuelle Maschine" in den *Systemvoraussetzungen auf Seite 1-2*, um weitere Informationen über den Typ der zur Installation erforderlichen virtuellen Maschine zu erhalten.

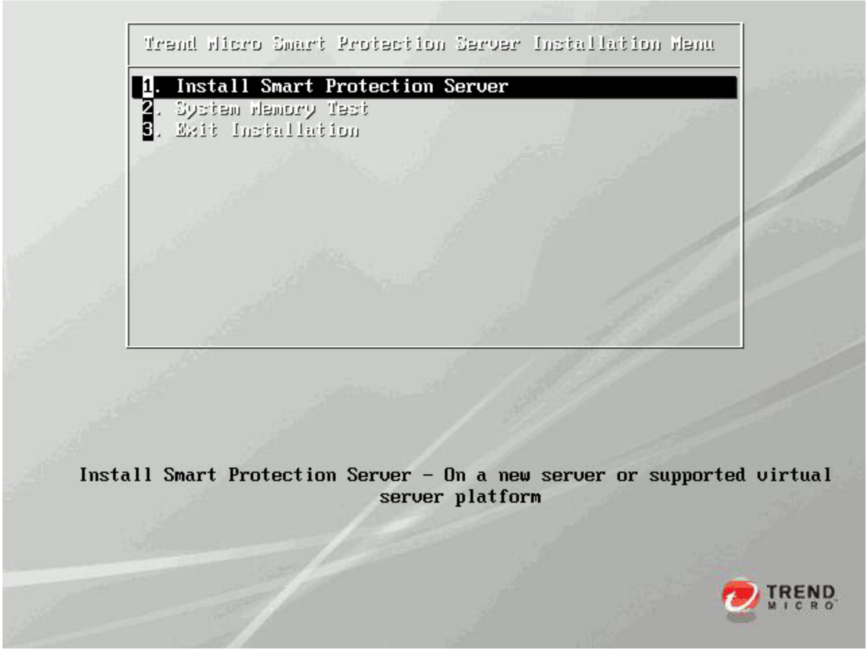
   Hinweis

   Ein physischer Netzwerkadapter ist zur Erkennung des Netzwerkgeräts für Hyper-V-Installationen erforderlich.

2. Schalten Sie die virtuelle Maschine ein.

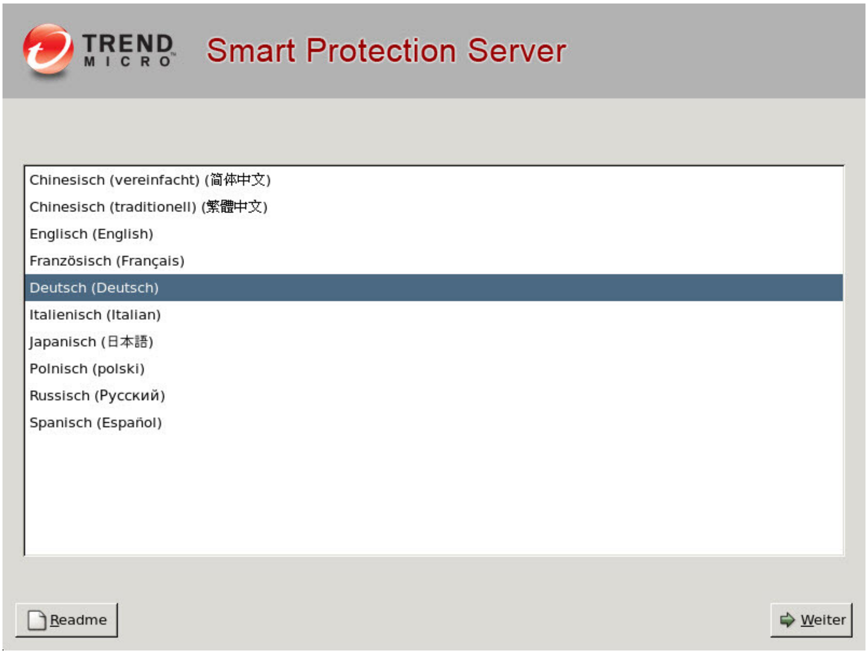
   Das Installationsmenü wird mit folgenden Optionen angezeigt:

   - **Smart Protection Server installieren:** Wählen Sie diese Option, um Smart Protection Server auf der neuen virtuellen Maschine zu installieren.
   - **Systemspeicher testen**: Wählen Sie diese Option, um den Arbeitsspeicher zu testen, um Probleme mit dem Arbeitsspeicher auszuschließen.
   - **Installation beenden**: Wählen Sie diese Option, um den Installationsvorgang zu beenden und das System von einem anderen Medium neu zu starten.



3. Wählen Sie **Smart Protection Server installieren**.

Das Fenster "Wählen Sie eine Sprache aus" wird angezeigt.

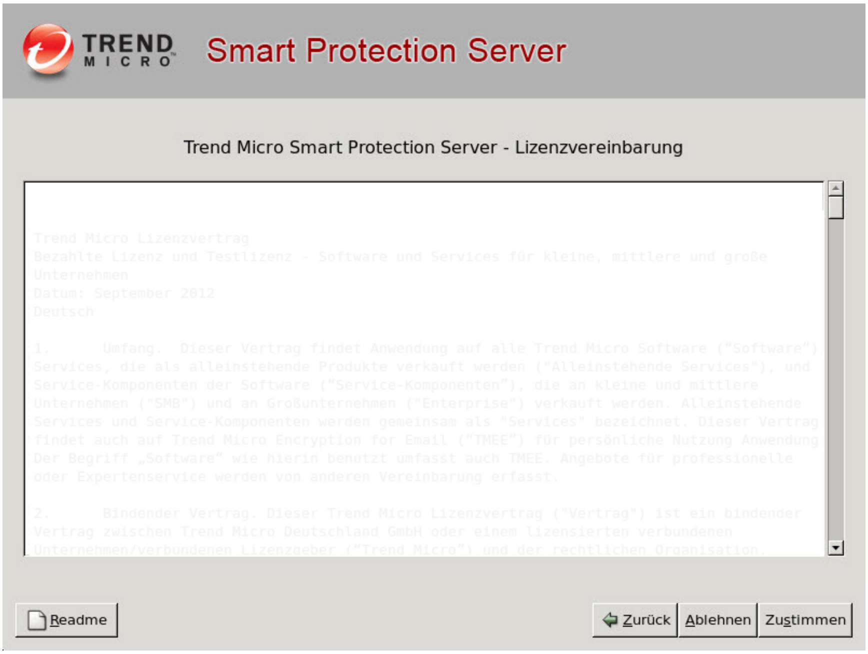


Hinweis

Von diesem Fenster aus können Sie über eine Schaltfläche, die sich in der linken unteren Ecke des Installationsfensters befindet, auf die Readme-Datei zugreifen.

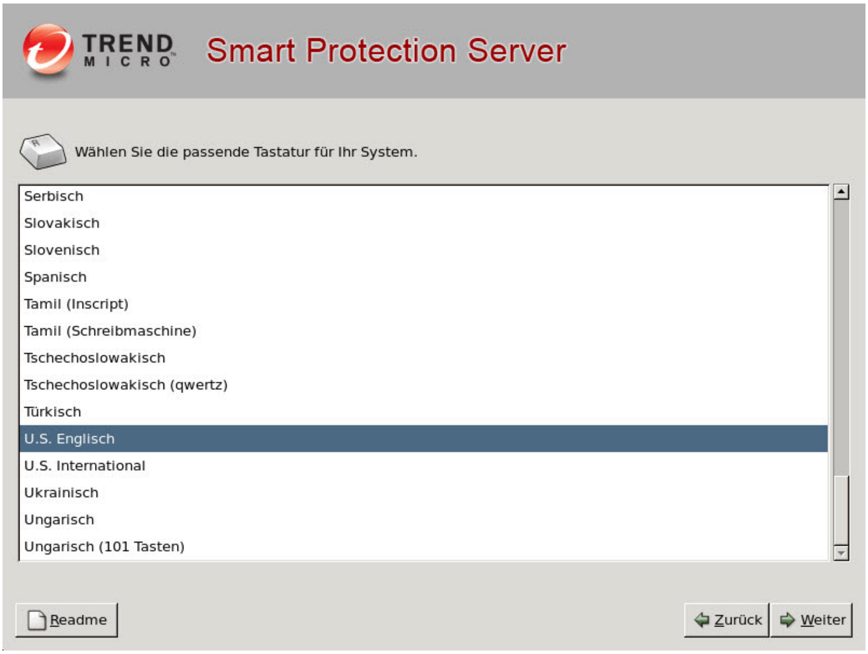
4. Wählen Sie die Sprache für diese Installation des Smart Protection Servers aus, und klicken Sie auf **Weiter**.

   Das Fenster "Lizenzvereinbarung" wird angezeigt.



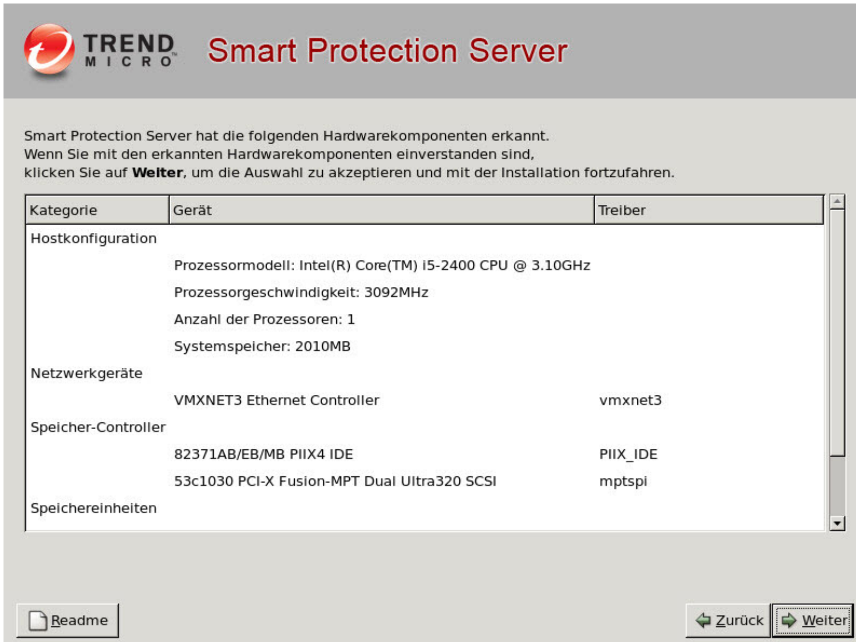
5. Klicken Sie auf **Zustimmen**, um fortzufahren.

   Das Fenster "Tastaturauswahl" wird angezeigt.



6. Wählen Sie die Tastatursprache, und klicken Sie auf **Weiter**, um fortzufahren.

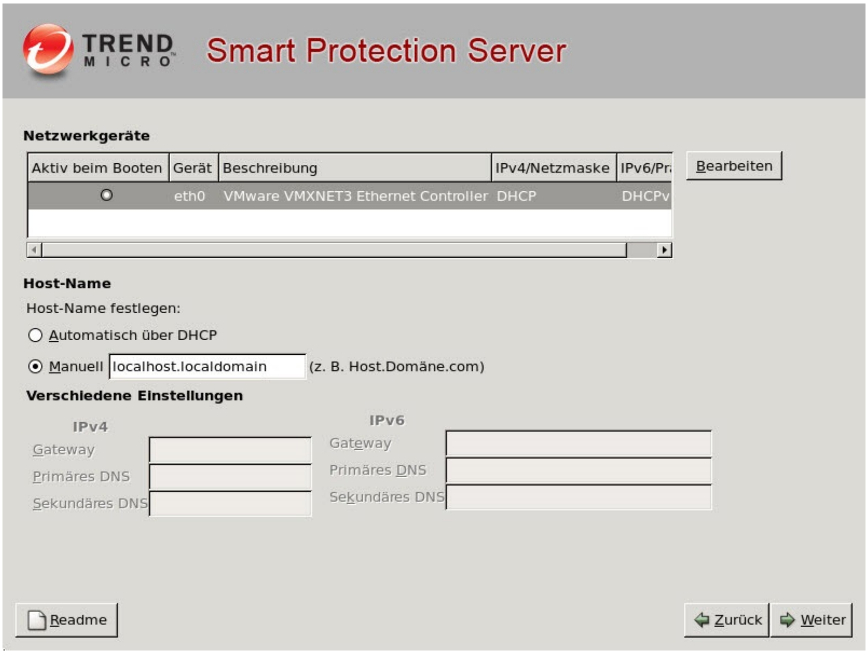
   Das Fenster "Zusammenfassung der Hardwarekomponenten" wird angezeigt.



Das Installationsprogramm führt eine Suche durch, um zu ermitteln, ob die Systemspezifikationen eingehalten werden, und zeigt die Ergebnisse an. Falls die Hardware Komponenten enthält, die nicht die Systemvoraussetzungen erfüllen, hebt das Installationsprogramm diese Komponenten hervor. Die Installation kann fortgesetzt werden, sofern eine Festplatte und ein Netzwerkgerät vorhanden sind. Falls keine Festplatte oder kein Netzwerkgerät vorhanden ist, kann die Installation nicht fortgesetzt werden.

7. Klicken Sie auf **Weiter**, um fortzufahren.

   Das Fenster "Netzwerkeinstellungen" wird angezeigt.



Hinweis

Um nach der Installation zu ändern, welches Gerät bei einem Neustart aktiv ist, melden Sie sich an der Befehlszeilenschnittstelle (CLI) an.

Falls mehrere Netzwerkgeräte vorhanden sind, konfigurieren Sie die Einstellungen für alle Geräte. (Beim Start darf nur ein Gerät aktiv sein.)

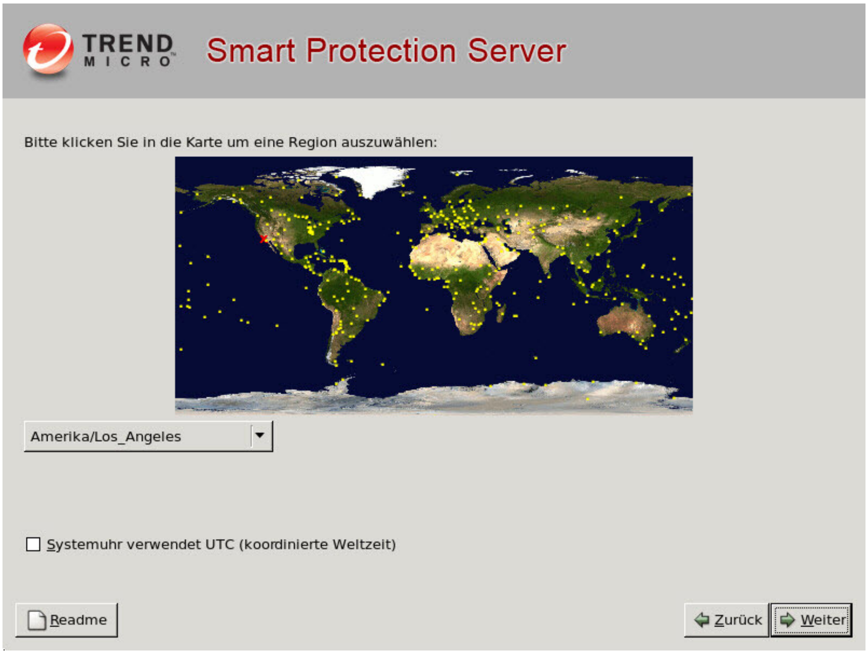
8. Geben Sie die Netzwerkgeräte an, die bei einem Neustart aktiv sind, sowie den Host-Namen und sonstige Einstellungen.

   Über die Schaltfläche **Bearbeiten** können Sie die IPv4- und IPv6-Einstellungen konfigurieren. Die Standardeinstellung für IPv4 ist die dynamische IP-Konfiguration (DHCP). Die Standardeinstellung für IPv6 ist DHCPv6.

9. Klicken Sie auf **Bearbeiten**, um die manuelle Konfiguration zu wählen und verschiedene Einstellungen zu konfigurieren.

10. Klicken Sie auf **Weiter**, um fortzufahren.

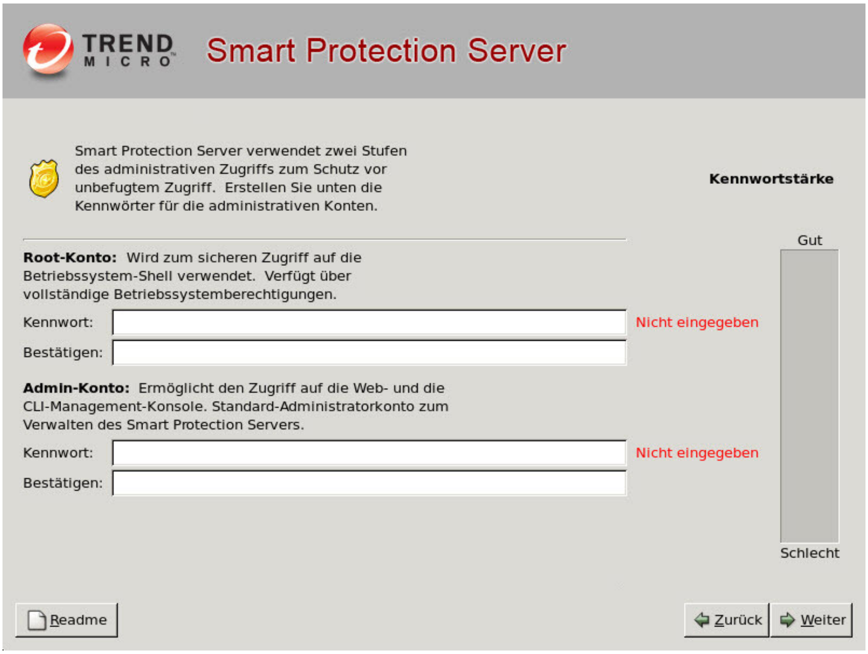
Das Fenster "Zeitzone" wird angezeigt.



11. Geben Sie die Zeitzone an.

12. Klicken Sie auf **Weiter**, um fortzufahren.

Das Fenster "Authentifizierung" wird angezeigt.



13. Geben Sie Kennwörter an.

Smart Protection Server verwendet zwei Stufen des administrativen Zugriffs, um den Server abzusichern: die Kennwörter **`root`** und **`admin`**.

- **Root-Konto:** Dieses Konto gewährt Zugriff auf das Betriebssystem und verfügt über alle Rechte für den Server. Dieses Konto umfasst die meisten Berechtigungen.
- **Admin-Konto:** Dieses Konto ist das Standard-Administrationskonto für den Zugriff auf die Web- und CLI-Produktkonsole von Smart Protection Server. Dieses Konto umfasst alle Rechte für den Smart Protection Server, aber keine Rechte für die Betriebssystem-Shell.

Hinweis

Das Kennwort muss zwischen 6 und 32 Zeichen lang sein. Beachten Sie Folgendes, wenn Sie ein sicheres Kennwort erstellen:

- Verwenden Sie sowohl Buchstaben als auch Ziffern.
- Vermeiden Sie Wörter, die in Wörterbüchern irgendeiner Sprache zu finden sind.
- Schreiben Sie Wörter absichtlich falsch.
- Verwenden Sie Phrasen oder kombinieren Sie Wörter.
- Verwenden Sie eine Kombination aus Groß- und Kleinschreibung.
- Verwenden Sie Sonderzeichen.

14. Klicken Sie auf **Weiter**, um fortzufahren.

    Das Fenster "Installationszusammenfassung" wird angezeigt.



15. Bestätigen Sie die Zusammenfassung.

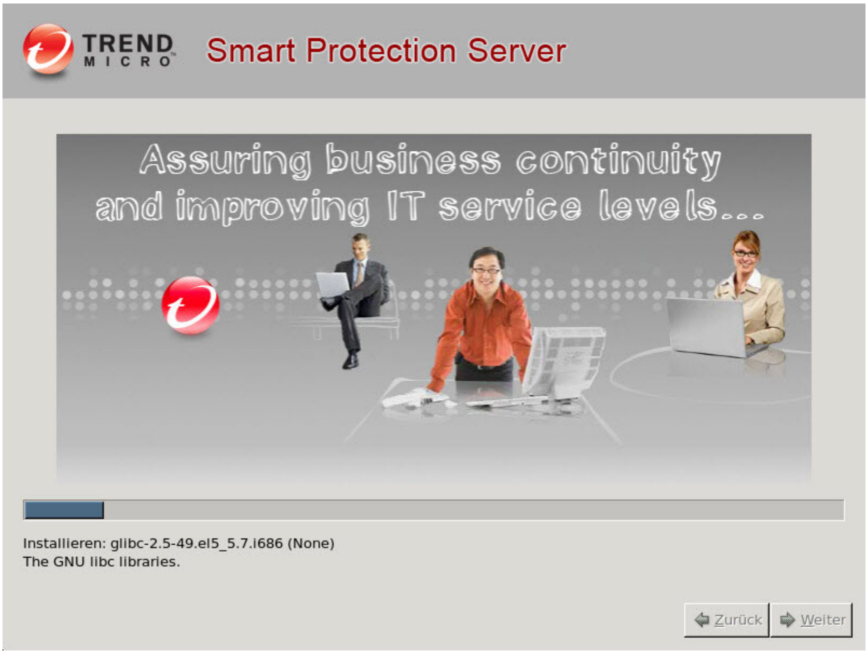
Hinweis

Wenn Sie mit der Installation fortfahren, wird der erforderliche Speicherplatz partitioniert und formatiert und das Betriebssystem und die Anwendung installiert. Wenn es Daten auf der Festplatte gibt, die nicht gelöscht werden sollen, brechen Sie die Installation ab, und erstellen Sie eine Sicherung, bevor Sie fortfahren.

Falls Sie im Fenster angezeigte Konfigurationsdaten ändern möchten, klicken Sie auf **Zurück**.

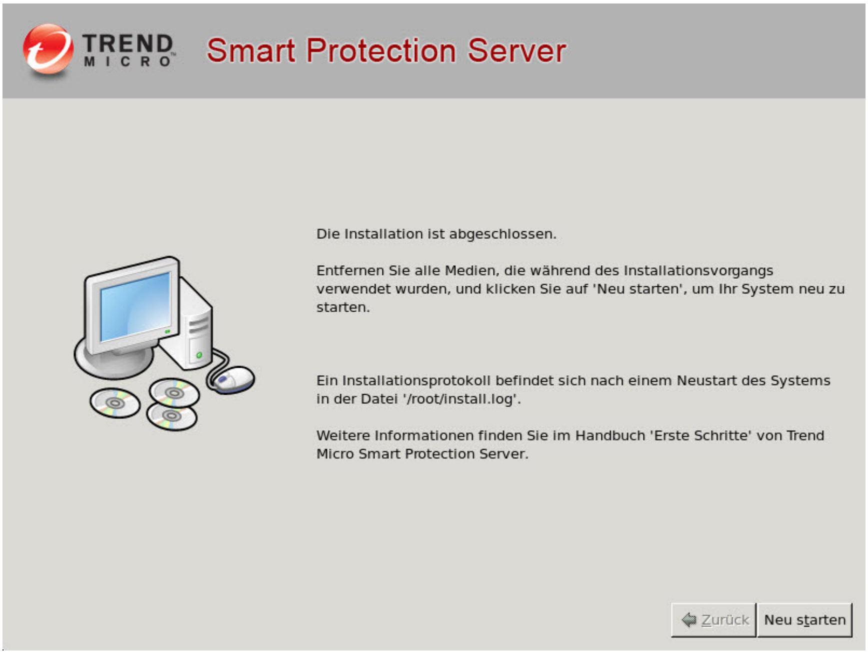
16. Klicken Sie auf **Weiter**, um fortzufahren, und auf **Fortsetzen**, wenn die Bestätigungsmeldung erscheint.

Das Fenster "Installationsfortschritt" wird angezeigt.



17. Wenn die Installation abgeschlossen ist, wird eine Meldung angezeigt.

Das Installationsprotokoll wird zu Referenzzwecken in der Datei `/root/install.log` gespeichert.



18. Klicken Sie auf **Neu starten**, um die virtuelle Maschine neu zu starten.

    Die anfängliche Anmeldeseite der Befehlszeilenschnittstelle (CLI) des Produkts erscheint und zeigt die Client-Verbindungsadressen und den URL der Webkonsole an.

    Hinweis

    Trend Micro empfiehlt, das CD-ROM-Laufwerk von der virtuellen Maschinen zu entfernen, nachdem Smart Protection Server installiert wurde.

19. Melden Sie sich als "admin" an der Produkt-CLI oder der Webkonsole an, um Smart Protection Server zu verwalten. Melden Sie sich an der Webkonsole an, um die Aufgaben durchzuführen, die nach der Installation erforderlich sind, wie beispielsweise das Konfigurieren der Proxy-Einstellungen. Melden Sie sich an der

CLI-Shell an, wenn Sie weitere Konfigurationsschritte, eine Fehlerbehebung oder Wartungsaufgaben durchführen möchten.

Hinweis

Sie können sich mit dem Konto `root` beim Betriebssystem anmelden, um alle Rechte zu erhalten.

20. Führen Sie die nach der Installation erforderlichen Aufgaben durch.

Einzelheiten finden Sie unter *Aufgaben nach der Installation auf Seite 3-1*.

Upgraden

Führen Sie ein Upgrade von Smart Protection Server 2.6, 2.5, 2.1 oder 2.0 auf diese Version von Smart Protection Server aus.

TABELLE 2-1. Versionsdetails für Upgrades

VERSION	VORAUSSETZUNGEN
Upgrade auf Smart Protection Server 3.0	• Stellen Sie vor der Installation sicher, dass die Systemvoraussetzungen eingehalten werden. Weitere Informationen finden Sie unter *Systemvoraussetzungen auf Seite 1-2*. • Smart Protection Server 2.0, 2.1, 2.5 oder 2.6 • Löschen Sie die temporären Internet-Dateien des Browsers, bevor Sie sich an der Webkonsole anmelden.

Der Web-Service wird während des Upgrade-Vorgangs für ungefähr 5 Minuten deaktiviert. Während dieser Zeit können Endpunkte keine Abfragen an den Smart Protection Server senden. Trend Micro empfiehlt während des Upgrades eine Umleitung der Endpunkte auf einen anderen Smart Protection Server. Wenn in Ihrem Netzwerk nur ein Smart Protection Server installiert ist, empfiehlt Trend Micro, das Upgrade bei geringem Netzaufkommen durchzuführen. Verdächtige Dateien werden sofort protokolliert und durchsucht, sobald die Verbindung zum Smart Protection Server wiederhergestellt wird.

Hinweis

SOCKS4-Proxy-Konfiguration wurde von Smart Protection Server entfernt. Falls in der vorherigen Version SOCKS4 für die Proxy-Einstellungen konfiguriert war, müssen die Einstellungen nach dem Durchführen eines Upgrades auf diese Version erneut konfiguriert werden.

Upgrade auf Smart Protection Server durchführen

Prozedur

1. Melden Sie sich an der Webkonsole an.
2. Klicken Sie im Hauptmenü auf **Updates**.

   Ein Menü wird angezeigt.
3. Klicken Sie auf **Programm**.

   Das Fenster "Programm" wird angezeigt.
4. Klicken Sie unter "Komponente hochladen" auf **Durchsuchen**.

   Das **Fenster zum Auswählen der hochzuladenden Datei** wird angezeigt.
5. Wählen Sie in diesem Fenster die Upgrade-Datei aus.
6. Klicken Sie auf **Öffnen**.

   Das Fenster zum Auswählen der hochzuladenden Datei wird geschlossen, und der Dateiname wird im Textfeld "Programmpaket hochladen" angezeigt.
7. Klicken Sie auf **Aktualisieren**.
8. Führen Sie die nach der Installation erforderlichen Aufgaben durch.

   Einzelheiten finden Sie unter *Aufgaben nach der Installation auf Seite 3-1*.

Kapitel 3

Aufgaben nach der Installation

Dieses Kapitel enthält Informationen über die erforderlichen Aufgaben nach der Installation von Trend Micro™ Smart Protection Server™.

Es werden folgende Themen behandelt:

Nach der Installation

Trend Micro empfiehlt, im Anschluss an die Installation folgende Aufgaben durchzuführen:

- Aktivieren Sie nach der Installation des Smart Protection Servers mit Hyper-V die Hyper-V-Integrationskomponente zur Erhöhung der Kapazität. Stellen Sie sicher, dass ein Netzwerkadapter verfügbar ist, bevor Sie die Hyper-V-Integrationskomponenten aktivieren. Aktivieren Sie die Hyper-V-Integrationskomponenten, indem Sie über die Befehlszeilenschnittstelle (CLI) Ihres Admin-Kontos Folgendes eingeben:

```
enable
enable hyperv-ic
```

- Wenn Sie mit den Mindestvoraussetzungen installiert haben, deaktivieren Sie das Protokoll "Gesperrter Internet-Zugriff" von der Befehlszeilenschnittstelle (CLI) aus, indem Sie im Admin-Konto Folgendes eingeben:

```
enable
disable adhoc-query
```

- Führen Sie die Erstkonfiguration durch. Siehe *Erstkonfiguration auf Seite 3-3*.
- Konfigurieren Sie die Einstellungen für den Smart Protection Server in anderen Trend Micro Produkten, die auf der intelligenten Suche basierende Lösungen unterstützen.

Hinweis

Im Echtzeit-Status-Widget und auf der CLI-Konsole des Smart Protection Servers werden die Adressen der Smart Protection Server angezeigt.

Nach der Installation von Smart Protection Server ist keine Installation von VMWare Tools mehr erforderlich. Das Kernel-Modul des Servers enthält das für den Smart Protection Server erforderliche VMWare Tools-Modul (vmxnet3).

Erstkonfiguration

Führen Sie folgende Aufgaben nach der Installation durch.

Prozedur

1. Melden Sie sich an der Webkonsole an.

   Der Assistent für die Erstinstallation wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen **"File-Reputation-Dienst aktivieren"**, um File Reputation zu verwenden.



3. Klicken Sie auf **Weiter**.

   Das Fenster "Web-Reputation-Dienst" wird angezeigt.

4. Aktivieren Sie das Kontrollkästchen **Web-Reputation-Dienst aktivieren**, um Web Reputation zu verwenden.



5. (Optional) Mit Hilfe der Einstellungen zur Filterpriorität können Sie die Filterreihenfolge für URL-Abfragen angeben.

6. Klicken Sie auf **Weiter**.

   Das Fenster "Smart Feedback" wird angezeigt.



7. Wählen Sie, ob Sie Smart Feedback verwenden möchten, um Trend Micro dabei zu unterstützen, schneller Lösungen für neue Bedrohungen bereitzustellen.

8. Klicken Sie auf **Weiter**.

   Das Fenster "Proxy-Einstellungen" wird angezeigt.



9. Geben Sie Proxy-Einstellungen an, falls in Ihrem Netzwerk ein Proxy-Server verwendet wird.

10. Klicken Sie auf **Fertig stellen**, um die Erstkonfiguration des Smart Protection Servers abzuschließen.

    Das Fenster "Zusammenfassung" der Webkonsole wird angezeigt.

> **Hinweis**
>
> Der Smart Protection Server aktualisiert die Pattern-Dateien nach der Erstkonfiguration automatisch.

Kapitel 4

Hilfe anfordern

In diesem Kapitel finden Sie Informationen, wie Sie beim Arbeiten mit Trend Micro™ Smart Protection Server™ zusätzliche Hilfe erhalten.

Es werden folgende Themen behandelt:

- *Support-Portal verwenden auf Seite 4-7*
- *Bedrohungsenzyklopädie auf Seite 4-8*
- *Kontaktaufnahme mit Trend Micro auf Seite 4-9*
- *TrendLabs auf Seite 4-10*

Häufig gestellte Fragen

Wie melde ich mich an der Befehlszeilenschnittstelle (CLI) an?

Mit Hilfe von CLI-Befehlen können Administratoren Konfigurationsaufgaben, Debugging und Fehlerbehebung durchführen.

Administratoren können sich mit dem **admin**-Konto über die SSH-Verbindung mit der CLI- oder SSH-Konsole an der Befehlszeilenschnittstelle anmelden.

Warum verschwindet die IP-Adresse des Smart Protection Servers, wenn ich die Hyper-V-Integrationskomponenten über die CLI auf einem nicht-Hyper-V-Computer aktiviere?

Microsoft™ Hyper-V-Integrationskomponenten sollten nur auf Microsoft™ Hyper-V-Computern aktiviert werden. Die IP-Adresse von Smart Protection Server wird nicht mehr angezeigt, wenn Hyper-V-Integrationskomponenten auf einem Nicht-Hyper-V-Computer aktiviert werden, wie hier gezeigt. Wenn Hyper-V-Integrationskomponenten

auf einem nicht-Hyper-V-Computer aktiviert werden, können Sie keine Verbindung zum Smart Protection Server über das Netzwerk herstellen.

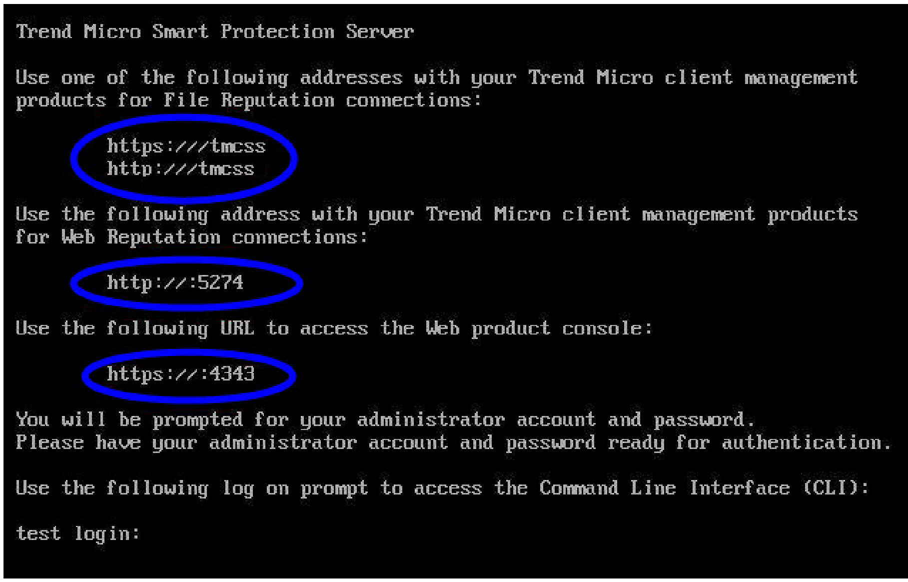


ABBILDUNG 4-1. IP-Adresse wird nicht mehr angezeigt

Hinweis

Auf Microsoft™ Hyper-V-Computern verschwindet möglicherweise die IP-Adresse, wenn ein Netzwerkadapter nicht angeschlossen ist.

Rollback der Netzwerkeinstellung ausführen

Prozedur

1. Melden Sie sich über die Befehlszeilenschnittstelle (CLI) unter **`admin`** an.

2. Geben Sie die folgenden Befehle ein:

```
enable
configure service interface eth0
```

Kann andere Linux-Software auf dem Smart Protection Server installiert werden?

Trend Micro empfiehlt nicht die Installation anderer Linux-Software auf der virtuellen Umgebung des Smart Protection Servers. Die Installation anderer Linux-Software kann die Leistung des Servers negativ beeinflussen, und andere Anwendungen funktionieren möglicherweise wegen der Sicherheitseinstellungen auf dem Smart Protection Server nicht ordnungsgemäß.

Wie kann ich die IP-Adresse des Smart Protection Servers ändern?

IPv4-Adresse ändern

Prozedur

1. Melden Sie sich über die Befehlszeilenschnittstelle (CLI) unter **`admin`** an.
2. Geben Sie die folgenden Befehle ein:

```
enable
configure ipv4 static <new ipv4 add> <subnet> <v4gateway>
```

3. Überprüfen Sie die Änderungen, indem Sie folgenden Befehl eingeben:

```
show ipv4 address
```

4. Starten Sie den Computer neu.

IPv6-Adresse ändern

Prozedur

1. Melden Sie sich über die Befehlszeilenschnittstelle (CLI) unter **`admin`** an.
2. Geben Sie die folgenden Befehle ein:

```
enable
configure ipv6 static <new ipv6 add> <prefix> <v6gateway>
```

3. Überprüfen Sie die Änderungen, indem Sie folgenden Befehl eingeben:

```
show ipv6 address
```

4. Starten Sie den Computer neu.

Wie kann ich den Hostnamen des Smart Protection Servers ändern?

Prozedur

1. Melden Sie sich über die Befehlszeilenschnittstelle (CLI) unter **`admin`** an.
2. Geben Sie die folgenden Befehle ein:

```
enable
configure hostname <hostname>
```

3. Überprüfen Sie die Änderungen, indem Sie folgenden Befehl eingeben:

```
show hostname
```

Wie führe ich ein Upgrade aus, wenn ein Pattern aktualisiert wird?

Trend Micro empfiehlt, vor dem Ausführen eines Upgrades abzuwarten, bis das Update eines Patterns abgeschlossen wurde. Deaktivieren Sie zeitgesteuerte Updates, um zu verhindern, dass ein Update während eines Upgrades ausgeführt wird.

Prozedur

1. Melden Sie sich über das **`admin`**-Konto an der Webverwaltungskonsole von Smart Protection Server an.
2. Klicken Sie auf **Updates** > **Pattern**.
3. Deaktivieren Sie zeitgesteuerte Updates.
4. Klicken Sie auf **Speichern**.

Hinweis

Denken Sie daran, nach dem Upgrade die zeitgesteuerten Updates wieder zu aktivieren.

Wie wird der NTP-Server konfiguriert?

Prozedur

1. Melden Sie sich über die Befehlszeilenschnittstelle (CLI) unter **`admin`** an.
2. Geben Sie die folgenden Befehle ein:

```
enable
configure ntp <ip or FQDN>
```

Support-Portal verwenden

Das Trend Micro Support-Portal ist täglich rund um die Uhr online verfügbar und enthält die aktuellsten Informationen zu häufig auftretenden und ungewöhnlichen Problemen.

Prozedur

1. Navigieren Sie zu http://esupport.trendmicro.com.
2. Wählen Sie in der entsprechenden Dropdown-Liste ein Produkt oder einen Dienst aus, und geben Sie sonstige entsprechende Informationen an.

   Die Seite **Technischer Support** wird angezeigt.
3. Verwenden Sie das Feld **Search Support** (Support suchen), um nach verfügbaren Lösungen zu suchen.
4. Falls keine Lösung gefunden wird, klicken Sie im linken Navigationsbereich auf **Submit a Support Case** (Support-Anfrage einreichen), und geben Sie die entsprechenden Informationen ein, oder reichen Sie eine Support-Anfrage auf der folgenden Seite ein:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   Ein Support-Mitarbeiter von Trend Micro analysiert Ihre Anfrage und antwortet innerhalb von maximal 24 Stunden.

Bekannte Probleme

Unter "Bekannte Probleme" werden unerwartete Eigenschaften des Produkts dokumentiert, für die möglicherweise eine vorübergehende Lösung erforderlich ist. Trend Micro empfiehlt, immer die Readme-Datei zu lesen, die Informationen über Systemvoraussetzungen und bekannte Probleme enthält, die die Installation oder die Leistung beeinflussen könnten. Readme-Dateien enthalten auch eine Beschreibung der neuen Funktionen einer Version sowie weitere, hilfreiche Informationen.

Die neuesten bekannten Probleme und mögliche Workarounds stehen auch in der Trend Micro Knowledge Base zur Verfügung:

http://esupport.trendmicro.com

Hotfixes, Patches und Service Packs

Nach der offiziellen Veröffentlichung eines Produkts erstellt Trend Micro oft Hotfixes, Patches und Service Packs zur Behebung besonderer Probleme, zur Leistungsverbesserung oder zur Funktionserweiterung.

Die folgende Übersicht zeigt, welche Komponenten möglicherweise von Trend Micro veröffentlicht werden:

- **Hot Fix**: Ein Workaround oder eine Lösung zu Problemen, über die Trend Micro von Kunden informiert wurde. Die von Trend Micro erstellten und veröffentlichten Hotfixes erhalten nur bestimmte Kunden.
- **Sicherheits-Patch**: Ein einzelner Hotfix oder eine Gruppe von Hotfixes zur Verteilung an alle Kunden.
- **Patch**: Eine Gruppe von Sicherheits-Patches zur Verteilung an alle Kunden.
- **Service Pack**: Eine erhebliche Funktionserweiterungen, die ein Upgrade des Produkts durchführt.

Ihr Händler bzw. Ihr Support-Anbieter informiert Sie ggf. bei Verfügbarkeit dieser Produkte. Weitere Informationen über neu veröffentlichte Hotfixes, Patches und Service Packs finden Sie auch auf der Trend Micro Website unter:

http://downloadcenter.trendmicro.com/?regs=DE

Jede Veröffentlichung enthält eine Readme-Datei mit Informationen über Installation, Verteilung und Konfiguration. Lesen Sie die Readme vor der Installation aufmerksam durch.

Bedrohungsenzyklopädie

Der Großteil der Malware besteht heutzutage aus "kombinierten Bedrohungen", also einer Kombination aus mindestens zwei Technologien zur Umgehung der Sicherheitsprotokolle des Computers. Trend Micro bekämpft diese komplexe Malware

mit Produkten, die eine benutzerdefinierte Verteidigungsstrategie verfolgen. Die Bedrohungsenzyklopädie enthält eine ausführliche Liste mit Namen und Symptomen von verschiedenen kombinierten Bedrohungen, wie etwa bekannte Malware, Spam, bösartige URLs und bekannte Schwachstellen.

Auf http://www.trendmicro.com/vinfo/de/virusencyclo/default.asp finden Sie weitere Informationen zu folgenden Themen:

- Malware und bösartige mobile Codes, die zum jeweiligen Zeitpunkt aktiv und im Umlauf sind
- Seiten mit Bedrohungsinformationen, die eine umfassende Ressource für Internet-Angriffe darstellen
- Beratung zu Internet-Bedrohungen bezüglich gezielten Angriffen und Sicherheitsbedrohungen
- Informationen zu Internet-Angriffen und Online-Trends
- Wöchentliche Malware-Berichte

Kontaktaufnahme mit Trend Micro

Trend Micro Mitarbeiter sind per Telefon, Fax oder E-Mail verfügbar:

Adresse	TREND MICRO INCORPORATED Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland
Telefon	+49 (0) 811 88990-700
Fax	+4981188990799
Website	http://www.trendmicro.com
E-Mail-Adresse	sales@trendmicro.de marketing@trendmicro.de

- Weltweite Support-Büros:

  http://www.trendmicro.de/ueber-uns/kontakt/index.html

- Trend Micro Produktdokumentation:

  http://docs.trendmicro.com/de-de/home.aspx

Problemlösung beschleunigen

Sie sollten die folgenden Informationen zur Hand haben, um die Problemlösung zu beschleunigen:

- Schritte, um das Problem nachvollziehen zu können
- Informationen zur Appliance und zum Netzwerk
- Marke und Modell des Computers sowie zusätzliche Hardware, die an den Endpunkt angeschlossen ist
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Betriebssystem- und Service Pack-Version
- Client-Version des Endpunkts
- Seriennummer oder Aktivierungscode
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventueller Fehlermeldungen
- Virtualisierungsplattform (VMware™ oder Hyper-V™) und Version

TrendLabs

Bei TrendLabs℠ handelt es sich um ein globales Netzwerk aus Forschungs-, Entwicklungs- und Wartungszentren, die täglich rund um die Uhr nach Sicherheitsbedrohungen suchen, Angriffe verhindern und schnell und problemlos Lösungen bereitstellen. TrendLabs dient als Backbone der Trend Micro Service-Infrastruktur und beschäftigt mehrere hundert Mitarbeiter und zertifizierte Support-Experten, die sich um die vielfältigen Anfragen zu Produkten und technischem Support kümmern.

TrendLabs überwacht die weltweite Bedrohungslage, um effektive Sicherheitsmaßnahmen anzubieten, mit denen Angriffe erkannt, vermieden und beseitigt werden können. Die Kunden profitieren von diesen täglichen Bemühungen in Form von häufigen Viren-Pattern-Updates und Erweiterungen der Scan Engine.

Weitere Informationen zu TrendLabs finden Sie unter:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Stichwortverzeichnis

TREND MICRO INCORPORATED
Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland
Tel.: +49 (0) 811 88990-700 Fax: +4981188990799
sales@trendmicro.de marketing@trendmicro.de

www.trendmicro.com

Item Code: APEM36293/140116